On relative primality and other properties of trinomials

Robert Dougherty-Bliss[1,*], Mits Kobayashi[1], Natalya Ter-Saakov[2] and Eugene Zima[3]

[1]Dartmouth College, Hanover, NH, USA
[2]Rutgers University, New Brunswick, NJ, USA
[3]University of Waterloo, Waterloo, Canada

Abstract
We discuss some properties of trinomial polynomials. These can be used to generate new balanced-size sets of moduli for accelerated modular arithmetic.

Keywords
Modular arithmetic, cyclotomic polynomials, resultant, dyadic rational.

1. Introduction

A popular technique to speed up computations with integer arithmetic is to reduce the input modulo several relatively prime numbers, compute with the residues, then reconstruct the result with the Chinese remainder theorem [3, 2, 5]. In [1], it was proposed to use "trinomial" moduli of the form

$$2^n - 2^k + 1, \quad 0 < k < n, \tag{1}$$

which are not only pairwise relatively prime, but also have pairwise scalable inverses. By that, we mean that replacing 2 with 2^c does not change the sparsity or bit-pattern of the modular inverses. For example, the moduli $2^{20} - 2^{12} + 1$ and $2^{20} - 2^4 + 1$ satisfy the following property: for any integer $c \geq 1$,

$$\begin{aligned} ((2^c)^{20} - (2^c)^{12} + 1)^{-1} &\equiv (2^c)^8 + 1 && \pmod{(2^c)^{20} - (2^c)^4 + 1)} \\ ((2^c)^{20} - (2^c)^4 + 1)^{-1} &\equiv (2^c)^{20} - (2^c)^{12} - (2^c)^8 + 1 && \pmod{(2^c)^{20} - (2^c)^{12} + 1)}. \end{aligned}$$

Using ad-hoc methods, the authors of [1] discovered a set of five pairwise relatively prime moduli of this form and used them in upper-layer on top of [2] to show improvement in a standard integer matrix multiplication benchmark.

Their work left open the following questions:

1. When are two trinomial moduli relatively prime?
2. Are there arbitrarily large sets of trinomial moduli with the same bit length?
3. For a fixed bit length, how can we efficiently find these sets?

Our aim is to answer some of these questions by examining the pure polynomial trinomials

$$x^n - x^k + 1, \quad 0 < k < n. \tag{2}$$

It seems reasonable to establish the relative primality of trinomial pairs of the form (2), then use this to deduce the relative primality of moduli of the form (1). Unfortunately, this does not work. Almost all pairs of trinomials of the form (2) are relatively prime over the rationals, yet only a small proportion of moduli of the form (1) are relatively prime integers. In other words, the substitution $x = 2$ in (2) does not preserve relative primality.

6^{th} *International Conference "Computer Algebra", Moscow, June 23–25, 2025*
*Corresponding author.
rdbliss@dartmouth.edu (R. Dougherty-Bliss); mits.kobayashi@dartmouth.edu (M. Kobayashi); natalya.tersaakov@rutgers.edu (N. Ter-Saakov); ezima@uwaterloo.ca (E. Zima)

Our results include a simple condition based on the resultant of two trinomials which ensures the relative primality of moduli of the form (1), a proof that arbitrarily large sets of relatively prime moduli exist, and some discussions on how to find such sets.

2. Dyadically resolving pairs

Definition 1. A pair of monic polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ *dyadically resolve* if their resultant is a signed power of 2.

If a pair of monic polynomials dyadically resolve, then they are relatively prime in $\mathbb{Q}[x]$. Their unique Bézout cofactors $a(x)$ and $b(x)$ with $\deg a < \deg g$ and $\deg b < \deg f$ in the equation

$$a(x)f(x) + b(x)g(x) = 1$$

will have dyadic coefficients. This is because the resultant is the determinant of the Sylvester matrix of $f(x)$ and $g(x)$, which is the coefficient matrix used to construct $a(x)$ and $b(x)$. The converse is also true, but it is not obvious.

Theorem 1. *The coefficients of the Bézout cofactors of $f(x)$ and $g(x)$ are all dyadic if and only if $f(x)$ and $g(x)$ dyadically resolve.*

If the trinomials $x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve then there exists an integer-coefficient polynomial $p(x)$ such that

$$\begin{gathered} \gcd(2^{cn} - 2^{ck} + 1, 2^{cn} - 2^{cj} + 1) = 1 \\ (2^{cn} - 2^{ck} + 1)^{-1} \bmod (2^{cn} - 2^{cj} + 1) = p(2^c) \end{gathered} \tag{3}$$

for sufficiently large positive integers c. In other words, the corresponding moduli that arise after setting $x = 2^c$ are relatively prime, and their inverses have a stable bit pattern.

We do not know of any simple, widely applicable condition that implies resolvability. For example, observe the sporadic behavior of powers of 2 in the following matrix.

$$\begin{pmatrix} 0 & 1 & 3 & 1 & 3 & 31 & 9 & 8 & 3 \\ 1 & 0 & 1 & 1 & 4 & 1 & 31 & 16 & 8 \\ 3 & 1 & 0 & 1 & 3 & 1 & 3 & 31 & 9 \\ 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 31 \\ 3 & 4 & 3 & 1 & 0 & 1 & 3 & 4 & 3 \\ 31 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \\ 9 & 31 & 3 & 1 & 3 & 1 & 0 & 1 & 3 \\ 8 & 16 & 31 & 1 & 4 & 1 & 1 & 0 & 1 \\ 3 & 8 & 9 & 31 & 3 & 1 & 3 & 1 & 0 \end{pmatrix}$$

Figure 1: $\operatorname{res}(x^{10} - x^i + 1, x^{10} - x^j + 1)$ for $1 \le i, j \le 9$.

As a first step to understanding these resultants, we report the following results.

Theorem 2. *As $n \to \infty$, there are arbitrarily large sets of trinomials of the form (2) which dyadically resolve pairwise.*

Our proof of this theorem is constructive, meaning that we can write down arbitrarily large sets at will. Unfortunately, the bit lengths used in our proof grow too quickly to be useful in practice. See Table 1.

size	exponents
1	{1}
2	{1, 2}
3	{2, 3, 4}
4	{12, 15, 16, 18}
5	{720, 760, 765, 768, 780}
6	{48372480, 48434496, 48435465, 48435712, 48436128, 48439664}

Table 1
Exponents constructed in the proof of Theorem 2. For each size, the given set consists of k such that the polynomials $x^n - x^k + 1$ dyadically resolve pairwise. The degree n is any fixed integer larger than the largest element of the set.

Theorem 3. *Let $i, j < n$ be positive integers.*

1. *$x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve if $k - j$ divides k.*
2. *$x^n - x^k + 1$ and $x^n - x^j + 1$ dyadically resolve if and only if $x^n - x^{n-k} + 1$ and $x^n - x^{n-j} + 1$ are.*
3. *If 2^v is the largest power of 2 that divides $k - j$, then $x^n - x^k + 1$ and $x^n - x^j + 1$ do not dyadically resolve if 2^v divides either k or $n - k$.*

There is a closed-form expression for the resultant of two binomials which has been known for many years (see [4]), but this is not true for trinomials. We can report a formula in a very special case.

Theorem 4. *If $k - j$ divides n, then*

$$\operatorname{res}(x^n - x^k + 1, x^n - x^j + 1) = \pm \left(\prod_{m \mid \frac{(k-l)}{\gcd(k,k-l)}} \Phi_m(2) \right)^{\gcd(k,k-l)}$$

where $\Phi_m(x)$ is the mth cyclotomic polynomial.

3. Relative primality

For a fixed n, almost all pairs of trinomials of the form (2) are relatively prime. In fact, if n is odd, then all of them are. The following theorem gives very strict conditions under which two trinomials can share a common factor over the rationals.

Theorem 5. *If $g(x) = \gcd(x^n - x^k + 1, x^n - x^j + 1)$ is not constant, then:*

1. *n is even;*
2. *$k - j$ is divisible by 6; and*
3. *$g(x)$ is a product of cyclotomic polynomials whose orders are multiples of 6.*

The preceding result shows that the only common factors two trinomials can have are cyclotomic polynomials. We can further describe exactly which cyclotomic polynomials divide which trinomials.

Theorem 6. *$\Phi_d(x)$ divides $x^n - x^k + 1$ if and only if d is a multiple of 6, and*

$$(n, k) \equiv \pm(d/3, d/6) \pmod{d}.$$

Using these results and some number theory, it is possible to show that roughly 97% of all pairs of trinomials for large even n are relatively prime.

4. Open questions

Our results answer some of the questions inspired by [1], but there remain open questions.

Minimal pairwise resolvability What is the smallest n such that there exists a set of k trinomials of the form (2) with degree n that dyadically resolve pairwise? The below table shows the first few values of this sequence.

set size k	smallest n
2	3
3	5
4	5
5	10
6	11
7	22
8	41
9	82
10	1668
11	???

Resultant of two trinomials Is there a formula for the resultant of two trinomials of the form (2) in terms of the cyclotomic polynomials evaluated at integers?

Fast construction of trinomial moduli What is the fastest way to construct large sets of pairwise dyadically resolving trinomials? Using maximal clique algorithms we have a method which is faster than a naive brute force approach, but there could be better ways.

Acknowledgments: We thank the Digital Research Alliance of Canada and the Office of Research Computing and Data Services at Dartmouth College for computational resources to run experiments.

References

[1] B. Chen, Y. Li, E. Zima, On a two-layer modular arithmetic, ACM Commun. Comput. Algebra 57 (2023) 133–136.

[2] J. Doliskani, P. Giorgi, R. Lebreton, E. Schost, Simultaneous conversions with the residue number system using linear algebra 44 (2018) 1–21. URL: https://dl.acm.org/doi/10.1145/3145573. doi:10.1145/3145573.

[3] D. E. Knuth, The Art of Computer Programming, Volume 2: Seminumerical Algorithms, Addison-Wesley Professional, 2014.

[4] R. Swan, Factorization of polynomials over finite fields, Pacific Journal of Mathematics 12 (1962) 1099–1106.

[5] E. V. Zima, A. M. Stewart, Cunningham numbers in modular arithmetic 33 (2007) 80–86. URL: http://link.springer.com/10.1134/S0361768807020053. doi:10.1134/S0361768807020053.